



UNITED STATES PATENT AND TRADEMARK OFFICE

A
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/734,777	12/12/2000	Antonius A.M. Staring	PHN 17,813	4699
24737	7590	12/05/2005	EXAMINER	
PHILIPS INTELLECTUAL PROPERTY & STANDARDS			DAVIS, ZACHARY A	
P.O. BOX 3001			ART UNIT	PAPER NUMBER
BRIARCLIFF MANOR, NY 10510			2137	

DATE MAILED: 12/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/734,777	STARING, ANTONIUS A.M.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 16 September 2005.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1,2,4-7 and 9-12 is/are rejected.
- 7) Claim(s) 3 and 8 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. The Examiner notes that Applicant has requested consideration of the reply under 37 CFR 1.116 received on 04 August 2005. However, this submission was previously considered as set forth in the advisory action mailed 22 August 2005. Because no amendments were made to the claims in the previous reply, it was considered merely as a request for reconsideration; therefore the reply was entered and considered, and such request and accompanying arguments were addressed in the advisory action. The Examiner further notes that no further arguments or amendments have been presented with the current request for continued examination in response to the Examiner's arguments set forth in the advisory action. No Claims have been amended, added, or canceled; Claims 1-12 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 04 August 2005 have been fully considered but they are not persuasive.

Claims 1, 2, 4-7, and 9-12 were rejected under 35 U.S.C. 103(a) as unpatentable over Komuro et al, US Patent 6223285, in view of Gray et al, US Patent 5706348.

Claim 1 is representative of the independent claims. The Examiner notes that Applicant has presented arguments that were submitted with the reply under 37 CFR 1.116 received 04 August 2005; however, this reply was already considered by the Examiner, as noted above. Because Applicant has not attempted to rebut the arguments set forth by the Examiner in the advisory action mailed 22 August 2005, Applicant's arguments are not considered persuasive. The Examiner's arguments are therefore repeated and expanded upon below, for Applicant's convenience.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Specifically, Applicant argues that Komuro does not teach decrypting a remaining encrypted part of the packet under control of a session key, based on the acknowledgement by the Examiner that Komuro does not disclose a key check block that is decrypted by candidate session keys until a valid result is obtained. The Examiner notes that Gray was relied upon for teaching the limitation of a key check block. Applicant further argues that the "EMI Extractor" of Komuro, which determines which key was used for encryption, "operates directly on the received data, before any decryption is performed" (see pages 7-8 of the response of 04 August 2005, referring to Figures 5A and 5B of Komuro), and that because it operates before decryption, it

cannot decrypt a remaining part. However, the Examiner additionally notes that the term “remaining encrypted part” does not exclude the entire packet as the remaining part, and therefore the argument is spurious because a remaining encrypted part (the entire packet) is decrypted in Komuro (column 10, lines 22-27).

Further, Applicant argues that Gray does not teach or suggest decrypting data of a received packet under control of a different one of the plurality of sink session keys until a valid decryption result is found. Specifically, Applicant argues that Gray does not test the validity of the decryption. The Examiner respectfully disagrees, noting that Gray explicitly states that it is determined whether the result of the decryption is valid (Figure 7, noting the results of decision block 106; see also column 6, lines 24-27). Applicant’s further arguments regarding the interpretation of Gray appear to be based on the above assertion that Gray does not test the validity of the decryption, and therefore are not further addressed.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 2, 4-7, and 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Komuro et al, US Patent 6223285, in view of Gray et al, US Patent 5706348.

In reference to Claim 1, Komuro discloses a secure communication system including a source device and at least one sink device, in which the source device includes a key generator that generates an active source session key at the initiative of the source device (column 9, lines 22-28) and an encryptor that encrypts at least part of a data field of a packet under control of the active source session key (column 9, lines 28-32); and in which the sink device includes a key generator that generates a plurality of candidate sink session keys, where for each index a respective sink session key corresponds to a respective source session key (column 10, lines 18-22); a decryptor that decrypts at least part of the data field of a received packet under control of a sink session key (column 10, lines 22-27); and a key resolver (column 10, lines 16-18) that determines which of the candidate source session keys used to encrypt a part of a received packet and causes the decryptor to decrypt a remaining encrypted part of the data field of the packet under control of the candidate sink session key (column 10, lines 22-27). However, Komuro does not explicitly disclose the generation of session keys in a predetermined sequence, nor does Komuro explicitly disclose the use of a key check block that is decrypted by the candidate sink session keys until a valid result occurs.

Gray discloses a network security system that includes generation of session keys in a predetermined sequence (column 2, lines 35-36) and a data field sub-field designated as a key check block field (column 5, lines 55-64). Gray further discloses

causing a decryptor to decrypt data in the key check block field under control of a different one of the plurality of candidate sink session keys until a valid decryption result is found (column 5, line 65-column 6, line 27). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Komuro by including the use of updating and checking keys periodically, in order to enhance security by reducing data security risks (see Gray, column 2, lines 35-36 and 47-51).

In reference to Claim 2, Gray further discloses that the plain-text form of the key check block is a public data block (column 5, lines 55-64).

In reference to Claim 4, Gray further discloses that the plain-text form of the key check block changes at least once during a communication session (column 2, lines 35-36 and 58-60).

In reference to Claim 5, Gray further discloses that the source and sink devices include corresponding key check block generators that generate and change the plain-text form of the key check block (column 4, lines 41-59; column 5, lines 55-64).

In reference to Claims 6 and 7, Gray further discloses that the plain-text form of the key check block of a particular packet is derived from information transferred in a packet preceding the particular packet (column 5, lines 7-13 and lines 40-64) and specifically in the packet immediately preceding the particular packet (column 5, lines 14-17 and 55-64).

Claim 9 recites limitations also recited in Claim 1, and is rejected by a similar rationale. Claims 10 and 11 are directed to methods corresponding substantially to the system of Claim 1 and the device of Claim 9, respectively, and are rejected by a similar rationale. Claim 12 is directed to a software implementation of the method of Claim 11, and is also rejected by a similar rationale.

Allowable Subject Matter

5. Claims 3 and 8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.
6. Reasons for indicating allowable subject matter in Claims 3 and 8 were set forth in the Office actions mailed 06 May 2004 and 13 January 2005.

Conclusion

7. All claims are drawn to the same invention claimed in the application prior to the entry of the submission under 37 CFR 1.114 and could have been finally rejected on the grounds and art of record in the next Office action if they had been entered in the application prior to entry under 37 CFR 1.114. Accordingly, **THIS ACTION IS MADE FINAL** even though it is a first action after the filing of a request for continued

Art Unit: 2137

examination and the submission under 37 CFR 1.114. See MPEP § 706.07(b).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Z. A. Davis
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad